14. (ONCE AMENDED) The data management method set forth in claim 8, wherein digital content distributors encrypt the encryption key employing a secret key, and the users decrypt the encrypted encryption key employing a public key provided in advance from the digital content distributors, using public key cryptography.

15. (ONCE AMENDED) The data management method set forth in claim 9, wherein digital content distributors encrypt the encryption key employing a secret key, and the users decrypt the encrypted encryption key employing a public key provided in advance from the digital content distributors, using public key cryptography.

16. (ONCE AMENDED) The data management method set forth in claim 1, wherein the sample data unit comprises as the invisible information a use count of times a user has used the digital content; characterized in that the invisible information is rewritten each time a user uses the digital content.

17. (ONCE AMENDED) The data management method set forth in claim 1, wherein the sample data unit comprises as the invisible information authorization information to enable use count control; characterized in that the invisible information is rewritten when a user uses the digital content a predetermined number of times and more.

REMARKS

STATUS OF CLAIMS

Claims 1-26 are pending.

Claims 1-6 and 16-26 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Yasukawa et al. (U.S. Patent No. 5,999,622) in view of Rhoads (U.S. Patent No. 6,343,138).

Claims 7-15 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Yasukawa and Rhoads in view of the applicants' own admission.

Claims 1-3, 5-17 are amended.

Thus, claims 1-26 remain pending for reconsideration, which is respectfully requested.

The foregoing rejections are traversed. No new matter has been added in this Amendment.

35 USC 103 REJECTIONS

The Examiner's primary assertion in the Response to Arguments and page 5 of the Office Action, appears to be that Yasukawa discloses encrypting a segment of a complete file and combining the encrypted data segments with the non-encrypted data segments, based on column 3, lines 65-67. However, Yasukawa only discloses a VBT flag indicating whether a file segment of a file is encrypted. Therefore, Yasukawa does not disclose the present invention's patentably distinguishing feature: "preparing a sample data ... wherein authorization information ... for accessing the encrypted digital content is embedded as invisible information in the sample data unit; and preparing synthesized data wherein the substantive data ... and the sample data are synthesized" (emphasis added).

In particular, the Examiner appears to be asserting that a segment of a complete file is same as the present invention's recited "sample data" of digital content. See also, Yasukawa, column 4, lines 16 to 29. Page 5 of the Office Action.

Further, the Examiner appears to be asserting that Yasukawa's VBT contains authorization information for accessing, such as decrypting, the encrypted content (Yasukawa, column 5, line 30 to column 7, line 54).

However, the Applicants request that the Examiner consider the recitation of independent claims 1, 25 and 26, as follows.

(1) First, Yasukawa is silent on the present invention's feature to embed invisible authorization information for accessing encrypted digital content in a sample data of the digital content and to synthesize the sample data with the encrypted digital content, because in Yasukawa the VBT only identifies the file segments that are encrypted by using a flag. Contrary to the Examiner's assertion on page 6 of the Action regarding claim 2, in Yasukawa, the decryption key for the encrypted file segments is separately provided to the user by a key distribution center (Yasukawa, column 4, lines 30-64). Therefore, Yasukawa's VBT flag is not an decryption key. Therefore, Yasukawa does not disclose or suggest the present invention's patentably distinguishing feature to provide with encrypted data authorization information for accessing the encrypted data (i.e., by watermarking authorization information for accessing encrypted content in a sample of the content). See operations 26 and 27 in FIGS. 2 and 4; and page 9, line 18 to page 11, line 4 of the Application.

Rhoads only relates to watermarking technology, and does not disclose or suggest using watermarking as "authorization information ... for accessing the encrypted digital content in the sample data" of the digital content, so that "sample data" can be synthesized with the encrypted data for distribution of the encrypted data.

To further emphasize that the current claim 1 recitation, "a content key employed as an encryption key when encrypting the digital content," differs from Yasukawa's flag indicating whether content is encrypted, independent claim 1 is amended as follows:

> ... extracting a portion of the digital content as sample data, and preparing a sample data unit wherein authorization information containing information for accessing the encrypted digital content is embedded as invisible information in the sample data unit; and
>
> preparing synthesized data wherein the substantive data unit and the sample data unit are synthesized, and distributing the synthesized data.

CLAIM 26

In contrast to Yasukawa, claim 26 expressly recites, "embedding content-authorization ... as a watermark in a sample of the content and synthesizing the sample with the content."

Claims 1-3, 5-17 are amended to be consistent with amended claim 1 and/or to improve recitation form. Support for the claim amendments can be found, for example, in operations 26 and 27 in FIGS. 2 and 4; page 3-7; page 9, line 18 to page 11, line 4; and page 17, line 15 to page 19, line 18 of the Application.

(2) Second, Yasukawa is silent on extracting a sample data unit from content data, because Yasukawa's reference to "segment" is a file segment corresponding to an actual portion of the physical media on which the file is stored (e.g., sectors on a CD-ROM, hard disk, a memory block, etc.) (Yasukawa, column 3, lines 39-52). In contrast to Yasukawa, the present invention's sample data is a sample (i.e., a representation) of content (page 13, lines 7-8 of the Application). A sample of content is used for additionally securing the content by watermarking the sample with authorization information used to access the content, such as providing a watermarked decryption key allowing decryption of encrypted content by the recipient without separately providing the decryption key to a user. Therefore, Yasukawa's "file segment" differs from the claim recitation, "sample data."

The Examiner asserts that "extracting a portion of the digital content" is obvious in view of Yasukawa encrypting only some file segments of the complete file (page 5 of the Action). However, the present invention's portion of the digital content differs from Yasukawa's selected file segments of a complete file, because a selected portion of the digital content is not tied to file segments but can be any arbitrary representation of the digital content, such as a frame image, etc. See, page 13, lines 7-17 of the Application.

(3) Third, regarding independent claim 25, the Examiner does not provide a rationale for the rejection. In contrast to Yasukawa, claim 25 provides: "a sample of the provider data having watermarked data-authorization information of the provider and a recipient." Yasukawa is completely silent on including recipient information in the VBT. The Examiner relies on Yasukawa for the data management configuration of the claimed present invention. However, in addition to Yasukawa's shortcoming by not disclosing invisible authorization information for accessing encrypted content in a sample of the encrypted content, Yasukawa also does not use recipient information in connection with file segment encryption and decryption.

Withdrawal of the rejection of claim 25 and allowance of claim 25 is respectfully requested.

(4) Fourth, regarding the Applicant's Admitted Related Art, the present invention's use of recipient information to protect data differs from the conventional techniques' use of recipient information to protect data. The prior art does not disclose or suggest the feature to embed invisible authorization information for accessing encrypted digital content in a sample data of the digital content and to synthesize the sample data with the encrypted digital content.

Claims 2-24 depending (directly or indirectly) from claim 1, recite patentably distinguishing features of their own and, further, are at least patentably distinguishing due to their dependencies from claim 1. In view of the amendments and the remarks, at least withdrawal of the finality of the action, or withdrawal of the rejections of claims 1-26 and allowance of claims 1-26, is respectfully requested.

CONCLUSION

Attached hereto is a marked-up version of the changes made to the claims by the current amendment. The attached page is captioned "**VERSION WITH MARKINGS TO SHOW CHANGES MADE**."

If there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

Respectfully submitted,
STAAS & HALSEY LLP

Date: May 6, 2003

By: _____
Mehdi D. Sheikerz
Registration No. 41,307

700 Eleventh Street, NW, Suite 500
Washington, D.C. 20001
(202) 434-1500

VERSION WITH MARKINGS TO SHOW CHANGES MADE

IN THE CLAIMS

Claims 1-3 and 5-17 are **AMENDED** as follows.

Recitation of all claims is provided for reference convenience.

1. (ONCE AMENDED) A data management method comprising:

preparing a substantive data unit by encrypting digital content that is for distribution;

extracting a portion of the digital content as sample data, and preparing a sample data unit wherein authorization information containing information for [a content key employed as an encryption key when encrypting]accessing the encrypted digital content is embedded as invisible information in the sample data unit; and

preparing synthesized data wherein the substantive data unit and the sample data unit are synthesized, and distributing the synthesized data.

2. (ONCE AMENDED) The data management method set forth in claim 1, [wherein use is enabled]further comprising:

enabling access to the synthesized data by separating the authorization information from the sample data unit[,]; and

restoring [the content]from the authorization information a decryption key for decrypting the substantive data unit [from said authorization information, and employing the content key to decrypt the substantive data unit into the original digital content].

3. (ONCE AMENDED) The data management method set forth in claim 1, wherein the sample data [being]is image data contained in the digital content and [wherein] at least one process among image processing, resizing, compressing and a γ-compensation is executed on the image data [contained in the digital content].

4. The data management method set forth in claim 1, wherein the sample data is index data for representing the substantive data unit.

5. (ONCE AMENDED) The data management method set forth in claim 4, wherein the synthesized data contains a plurality of substantive data units based on a plurality of digital content items, and contains a plurality of sample data units corresponding to the plurality of

substantive data units; and wherein each sample data [constituting the plurality of sample data units] is linked with respective corresponding ones of the plurality of substantive data units.

6. (ONCE AMENDED) The data management method set forth in claim 1, wherein the sample data units [are]is data structuralized in one of JPEG and MPEG formats, and

the synthesized data is prepared by add-on synthesizing the substantive data unit to the sample data unit using the format of the sample data unit.

7. (ONCE AMENDED) The data management method set forth in claim 1, wherein [the authorization information being information wherein the content key is encrypted, with] the encryption key [being]is at least one of user identification information, equipment identification information loaded in user-employed computers, CPU identification information loaded in the user-employed computers, and identification information unique to digital-content-storing recording media.

8. (ONCE AMENDED) The data management method set forth in claim 1, wherein [the authorization information being information wherein the content key is encrypted, with] the encryption key [being]is identification information common to a plurality of users.

9. (ONCE AMENDED) The data management method set forth in claim 1, wherein [the authorization information being information wherein the content key is encrypted, with] the encryption key [being]is at least one of identification information unique to distributors of the digital content, and identification information unique to authors of the digital content.

10. (ONCE AMENDED) The data management method set forth in claim 7, wherein a decryption key for decrypting the encrypted [content]encryption key is [in] common [with the]to an encryption key for encrypting the digital content, the decryption key being a shared key based on exclusive information transmitted and received among users and content distributors, using symmetric cryptography.

11. (ONCE AMENDED) The data management method set forth in claim 8, wherein a decryption key for decrypting the encrypted [content] encryption key is [in] common [with the]to an encryption key for encrypting the digital content, the decryption key being a shared key

based on exclusive information transmitted and received among users and content distributors, using symmetric cryptography.

12. (ONCE AMENDED) The data management method set forth in claim 9, wherein a decryption key for decrypting the encrypted [content]encryption key is [in] common [with the]to an encryption key for encrypting the digital content, the decryption key being a shared key based on exclusive on exclusive information transmitted and received among users and content distributors, using symmetric cryptography.

13. (ONCE AMENDED) The data management method set forth in claim 7, wherein [the] digital content distributors encrypt the [content]encryption key employing a secret key, and the users decrypt the encrypted [content]encryption key employing a public key provided in advance from the digital content distributors, using public key cryptography.

14. (ONCE AMENDED) The data management method set forth in claim 8, wherein [the] digital content distributors encrypt the [content]encryption key employing a secret key, and the users decrypt the encrypted [content]encryption key employing a public key provided in advance from the digital content distributors, using public key cryptography.

15. (ONCE AMENDED) The data management method set forth in claim 9, wherein [the] digital content distributors encrypt the [content]encryption key employing a secret key, and the users decrypt the encrypted [content]encryption key employing a public key provided in advance from the digital content distributors, using public key cryptography.

16. (ONCE AMENDED) The data management method set forth in claim 1, wherein the sample data unit comprises as the invisible information a use count of times a user has used the digital content; characterized in that the invisible information is rewritten each time a user uses the digital content.

17. (ONCE AMENDED) The data management method set forth in claim 1, wherein the sample data unit comprises as the invisible information authorization information to enable use count control; characterized in that the invisible information is rewritten when a user uses the digital content a predetermined number of times and more.

18. The data management method set forth in claim 16, characterized in that the invisible information is rewritten on decrypting and reading the substantive data unit.

19. The data management method set forth in claim 16, characterized in that the invisible information is rewritten when use of the digital content is ended.

20. The data management method set forth in claim 17, characterized in that the invisible information is rewritten on decrypting and reading the substantive data unit.

21. The data management method set forth in claim 17, characterized in that the invisible information is rewritten when use of the digital content is ended.

22. The data management method set forth in claim 16, wherein the invisible information in the sample data unit comprises an error recovery function by containing redundant information.

23. The data management method set forth in claim 16, characterized in that limits on read-out and use in decrypting the substantive data unit are governed based on the invisible information in the sample data unit.

24. The data management method set forth in claim 16, characterized in that one of year, month, date, and time limits within which read-out and use is possible in decrypting the substantive data unit are governed based on the invisible information in the sample data unit.

25. A computer data signal embodied in a carrier wave, comprising provider data synthesized with a sample of the provider data having watermarked data-authorization information of the provider and a recipient, thereby allowing a recipient system to access the data according to the synthesized data-authorization information.

26. A computer, comprising:

a programmed computer processor embedding content-authorization information as a watermark in a sample of the content and synthesizing the sample with the content.